Remarks/Arguments

This application has been reviewed in light of the Final Office Action dated March 4, 2009. Claims 1-13 are currently pending and stand rejected. Claims 1, 6, 8-10, and 13 are independent. Claims 1 and 9 are amended to clarify certain aspects of the claim language. No new matter has been added. Reconsideration of the claim rejections is requested.

Rejections under 35 U.S.C. 102 (e)

Claims 1, 4-6, 8-10, and 13 are rejected under 35 U.S.C. 102 (e) as allegedly being anticipated by Marsh (U.S. Patent No. 7,080,039). Applicants respectfully assert that for at least the reasons discussed below claims 1, 4-6, 8-10, and 13, are not anticipated by Marsh.

Marsh is directed to systems and methods for associating media content with households using smart cards. Marsh teaches using household identifiers on smart cards in order to encrypt or decrypt media content. Marsh does not, however, teach or suggest each and every limitation of Applicants' independent claims 1, 4-6, 8-10, and 13. Each independent claim is discussed below.

Claim 1

A review of the "Response to Arguments" section of the final Office action, pages 2 and 3 and the final Office action pages 7-9 finds that the Office appears to be making several conclusory statements that every claimed feature, except for the processor and second port, is equivalent to the smart card of Marsh and that the second port equates with the smart card reader and the processor with the module 222 of Marsh.

Claim 1 clearly recites a removable digital memory including a port at which digital information stored on said removable digital memory can be accessed; a memory for storing first conditional access data and at least one content encryption key; a second port for receiving user certificate data and a first key of a key pair contained in an access card.

In responding to applicants' prior argument that Marsh does not teach or suggest a device comprising, inter alia, "memory for storing first conditional access data and at least one content encryption key." The Examiner stated that Marsh discloses conditional access data in the form of a certificate and also alleged that Marsh discloses that the smart card holds a pair of keys. The smart card transmits to the module a key to be used for encryption.

-7-

However, applicants' claim 1 also recites that a processor is responsive to the user certificate data received on said second port for authenticating the received certificate data based on the first conditional access data stored in said memory, the processor, upon said authentication, encrypting information stored in said removable digital memory using the at least one content encryption key, to thereby provide encrypted information in said removable digital memory, the processor operable for encrypting said content encryption key using said first key received on said second port and outputting said encrypted content encryption key to enable access of said encrypted information stored on said removable digital memory by an external device.

Nowhere does Marsh suggest that the module 222 outputs an encrypted content encryption key to enable access of encrypted information stored on the smart card 246 by an external device. Thus, Marsh does not teach the recited feature of outputting said encrypted content encryption key to enable access of said encrypted information stored on said removable digital memory by an external device.

Furthermore, the Office Action states that the claimed second port is equated to the smart card reader, however claim 1 recites a second port for receiving user certificate data. The Office Action states that the claimed conditional access data is the same as Marsh's certificate. But the Office Action never mentions applicant's claimed feature of the second port for receiving user certificate data (see pages 8 and 9 of the final Office action).

In addition, in discussing the "processor" feature on page 9 of the final Office action the Office appears to be combining the claimed user certificate data with the certificate data as all being equivalent to Marsh's certificate. Marsh states that each certificate is a self-signed certificate. Nowhere does Marsh or the Office action mention the user certificate data nor is there any suggestion of the claimed feature that the processor is responsive to the user certificate data received on said second port for authenticating the received certificate data based on the first conditional access data stored in said memory.

Also claim 1 recites:

a memory for storing first conditional access data and at least one content encryption key;

a second port for receiving user certificate data and a first key of a key pair contained in an access card.

-8-

Customer No. 24498
Attorney Docket No. PU030342
Office Action Date: March 4, 2009

On page 8 of the final Office action the recited content encryption key is alleged to correspond to the public key of key pair 270. Then with regard to the claimed second port and the first key of a key pair contained in an access card, the Office fails to mention this feature.

Marsh clearly fails to show each and every recited feature and the rejection should be withdrawn. Therefore, for at least the foregoing reasons, claim 1 is believed to be not anticipated by Marsh.

Claim 6

Marsh does not teach or suggest an access card comprising, "memory, following authentication of said card with a destination device, being <u>updated</u> to store a public key of a public/private key pair stored in said destination device," as recited in claim 6. Emphasis added.

The Final Office Action at page 3 alleges that "memory, following authentication of said card with a destination device, is updated to store a public key of a public/private key pair stored in said destination device," as recited in claim 6 is disclosed by Marsh, wherein after authentication of the smart card takes place, the module transmits the public key to the smart card for decryption of data. The Final Office Action also points to Marsh at col. 10, lines 52-61 as disclosing this feature of claim 6. Applicants respectfully disagree.

Marsh, at col. 10, lines 47-51, states "upon receiving the challenge once, smart card 246 responds to the challenge by digitally signing the received random number using the private key of key pair 270. This signed number is then returned to module 222 as the response." At col. 10, lines 52-61, Marsh states "The response is verified using the public key of key pair 270, which is known to module 222. . . . As only smart card 246 knows the private key of key pair 270, the module 222 can verify the authenticity of smart card 246 by evaluating, using the public key of key pair 270."

Marsh, however, does not disclose that the access card memory is "<u>updated</u> to store a public key of a public/private key pair stored in said destination device" as recited in claim 6. Emphasis added. Applicants respectfully repeat this argument as presented in the response dated November 14, 2008 on pages 14-15.

Therefore, for at least the foregoing reasons, Marsh does not teach or suggest claim 6 for at least the above reasons.

-9-

Customer No. 24498
Attorney Docket No. PU030342
Office Action Date: March 4, 2009

Claim 8

Marsh does not disclose or suggest a digital information destination device comprising, inter alia, "memory preloaded with at least a second stored User Certificate and mutually corresponding private and public encryption keys associated with said destination device," as recited in claim 8. Emphasis added.

The Final Office Action at page 4 notes that the module 220 receives a certificate from the certificate authority consisting of a public/private key pair. Fig. 4 of Marsh is also cited as teaching this element. Applicants respectfully disagree and reiterate the argument as presented in the response dated November 14, 2008 on pages 15-16, that all of the content encryption keys in Marsh are originally stored in memory on the smart card, not on the device into which the smart card is inserted. As a result, claim 8 is believed to be patentable over Marsh for at least the above-mentioned reasons.

Claim 9

For the reasons discussed above with reference to claim 1, it is clear that Marsh fails to teach or suggest all the features recited in claim 9. Please refer to the remarks for claim 1.

Claim 10

For at least the reasons discussed above with reference to claim 1, it is clear that Marsh fails to disclose or suggest all the features as recited in claim 10. Applicant's essentially repeat the above arguments from claim 1 to explain why claim 10 is different from Marsh.

In addition, Marsh does not teach or suggest a method which includes "placing said access card in said access card port of said destination device" for authentication and "writing said public encryption key from said destination device to said access card" prior to placing the access card in the source device of the media.

The Final Office Action at page 6 alleges that Marsh discloses this feature at col. 10, lines 47-51, which recites "upon receiving the challenge nonce, smart card 246 responds to the challenge by digitally signing the received random number using the private key of key pair 270. This signed number is then returned to module 222 as the response." However, Applicants respectfully note that Marsh does not disclose that module 222 transmits the public key to the smart card 246. Applicants respectfully repeat the argument as presented in the response dated November 14, 2008 on pages 16-17, that the encryption keys in Marsh originate from the access card. As such, Marsh does not disclose "writing said public encryption key from said destination

-10-

device to said access card" as recited in claim 10.

Furthermore, as discussed with reference to claim 6, authenticating the access card with the destination device and transferring an encryption key from the destination device to the access card before inserting the card into the source device provides enhanced security that are not contemplated by Marsh. Thus, Marsh clearly does not teach or suggest claim 10. As such, claim 10 is believed to be patentable over Marsh.

Claim 13

Marsh does not disclose or suggest an "access card comprising: a memory having at various times at least first, second, and third states...," as recited in claim 13. The Final Office Action at page 6 alleges that Marsh discloses that authentication takes place between the module and the smart card using a challenge. As cited above, March, at col. 10, lines 47-51, recites "upon receiving the challenge nonce, smart card 246 responds to the challenge by digitally signing the received random number using the private key of key pair 270. This signed number is then returned to module 222 as the response." Marsh, at col. 8, lines 2-5, appears to teach that "a public key/private key pair may still be stored on smart card 246 for authentication purposes." However, Applicants respectfully note that Marsh <u>does not</u> disclose that module 222 transmits the public key to the smart card 246. Applicants respectfully reiterate the argument as presented in the response dated November 14, 2008 on pages 17-18 that in Marsh, it is the <u>smart card</u> that holds the user certificates and encryption keys, not the destination and source devices. Thus, it is clear that Marsh does not disclose or suggest the access card having various states claimed in claim 13.

Since, Marsh fails to teach or suggest all of the aspects of claims 1, 6, 8-10, and 13, these claims are believed to be patentable over Marsh. Accordingly, Applicants assert that claims 1, 6, 8-10, and 13 are in condition for allowance for at least the stated reasons. Additionally, applicants respectfully assert that claims 4-5 are patentable over Marsh at the very least by their dependence from claim 1. Reconsideration of the rejections is earnestly solicited.

Rejections under 35 U.S.C. 103 (a)

Claims 2, 3, 7, 11 and 12 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Marsh in view of Roskind (U.S. Patent Publication 2003/00466544). Since claims 2, 3, 7, 11 and 12 depend from claims 1, 6 and 10, applicants assert that these claims are patentable over Marsh

-11-

for at least the same reasons described above.

Roskind does not cure the deficiencies of Marsh in this regard. Roskind is directed to a digital certificate with a limited useful life. Roskind does not disclose systems and methods for encryption and decryption of media content, as recited in Applicants' pending claims. Roskind only teaches systems and methods for authentication of certificates. As such Roskind does not remotely suggest any of the above deficiencies of Marsh. Therefore, claims 2, 3, 7, 11 and 12 are believed to be patentable over the combination of Marsh and Roskind. Reconsideration of the obviousness rejection is requested.

Since the cited art fails to disclose or suggest all of the features of independent claims 1, 6, 8-10 and 13, these claims are believed to be patentable over Marsh and Roskind, taken singly or in combination. Accordingly, applicants respectfully assert that the above-mentioned claims are in a position for allowance for at least the stated reasons. Additionally, applicants respectfully assert that claims 2, 3, 7, 11, and 12 are patentable over Marsh and Roskind at least by virtue of their respective dependencies from the aforementioned independent claims. Reconsideration of the rejections is earnestly solicited.

Customer No. 24498
Attorney Docket No. PU030342
Office Action Date: March 4, 2009

Conclusion

In view of the foregoing remarks, it is respectfully submitted that all claims now pending in the application are in condition for allowance. Early and favorable reconsideration of the case is respectfully requested. If the Examiner cannot take such action, the Examiner should contact the applicant's attorney at (609) 734-6815 to arrange a mutually convenient date and time for a telephonic interview.

In the event that there are any errors with respect to the fees for this response or any other papers related to this response, the Director is hereby given permission to charge any shortages and credit any overcharges of any fees required for this submission to Deposit Account No. 07-0832.

Respectfully submitted,
Gervais, et al.

By: _____

Paul P. Kiel
Reg. No. 40,677
(609) 734-6815

Date: 5/7/09

Patent Operations
Thomson Licensing LLC
P.O. Box 5312
2 Independence Way
Princeton, NJ 08543-5312

-13-